CVE-2016-6484

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-6484
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2018-10-09 20:00:00 UTC
Description	CRLF injection vulnerability in Infoblox Network Automation NetMRI before 7.1.1 allows remote attackers to inject arbitrary

Risk And Classification

Problem Types: CWE-93

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Infoblox	Netmri	All	All	All	All

References

Reference
Infoblox Network Automation CVE-2016-6484 HTTP Response Splitting Vulnerability
SecurityFocus
Infoblox 7.0.1 CRLF Injection / HTTP Response Splitting ≈ Packet Storm
NetMRI Input Validation Flaws Let Remote Users Conduct Cross-Site Request Forgery, HTTP Response Splitting, and Cross-Site Scripting At
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report